

Article

Discrimination by Design: predictive data mining as security practice in the United States' 'war on terrorism'

Keith Guzik

Bloomfield College, USA. keithguzik@gmail.com

Abstract

The tactics and strategies employed by the United States in its 'War on Terrorism' have generally been condemned as departures from the norms of how a democratic government conducts itself. Reforms are thus thought needed to place the 'War on Terror' under the rule of law and protect civil liberties. This article attempts to counter that view. Using predictive data mining—a technology at the heart of the US National Security Agency's (NSA) surveillance scandal—as an example, it argues that rather than a break with the past, the tactics that the Bush Administration adopted to fight terrorism represent an extension of a particular type of future-oriented power which Foucault (2008) referred to as "security" or "government." And while individual civil liberties are no doubt at stake, they are not at stake equally for everyone. Predictive data mining discriminates by design, designating certain groups as threats relative to others. Thus, persons with Middle Eastern and North African backgrounds will disproportionately bear the burden of this surveillance technique and the innumerable mistakes it produces. Finally, the rule of law would seem to offer little to remedy the situation. The War on Drugs, the policing of immigration, and past international disputes with 'terrorist regimes' have provided a "crime jurisprudence" (Simon 2007) that legitimizes such discrimination. Paradoxically and pessimistically then, the real hope for change lies in the crisis of legitimacy that one could expect to result from the wider application of such discriminatory technologies or the benevolent reign of an executive branch that has been imbued with an authority beyond its traditional limits.

Introduction

The practices, places, and technologies operant in the United States' 'War on Terrorism'—"enemy combatants," "black sites," "warrantless wiretapping," "waterboarding," "extraordinary rendition," etc.—have passed into the popular vocabulary and imagination. Harold and Kumar now scheme to escape Guantanamo rather than score steamed Slider burgers in suburban New Jersey. For scholars interested in surveillance and socio-legal issues, the wider public engagement with such topics as **civil liberties, international law, and government surveillance** provides a unique opportunity to contribute to and influence public discourse on counterterrorism policy.

One example of socio-legal scholars seizing this opportunity has been the on-going discussion, born in the twilight of the Bush Administration, of how to best handle the ongoing 'War on Terrorism.' David Cole and Jules Lobel (2007), for instance, argue that the Bush Administration's use of "anticipatory state

violence” to prevent¹ acts of terrorism fell outside the “rule of law.” Thus, the government should return to its previous legal framework—obtaining Foreign Intelligence Surveillance Act (FISA) bench warrants to conduct surveillance on suspicious persons and using traditional police work to disrupt terrorist plots—to fight terrorism (247-259). Jack Goldsmith (2007), who briefly served as head of the Justice Department’s Office of Legal Counsel (OLC) under President Bush, sees the problem with the US response to terrorism as more political than legal—Congress and the public were not adequately consulted during the implementation of the counterterrorism policies—and argues that new dialogue and institutions, such as a “national-security court” (Goldsmith 2008), would strengthen such efforts. For his part, Bruce Ackerman (2006) offers both the most reasonable analysis of the situation—we are fighting neither a “war” nor “crime”—and the most radical solution—an “emergency constitution” that would provide the president temporary emergency powers to deal with the aftermath of terrorist attacks.

However disparate these positions first appear, the discussion on the path forward in the ‘War on Terrorism’ possesses more agreement than not. The contours of consensus include a few basic ideas. First, the practices and policies of the Bush Administration represented *departures from the norm* of how a modern, democratic government should police criminal activities and how the United States government has done so in the (immediate) past². Second, these departures pose a *threat to civil liberties* in the country. And third, to prevent this abuse from becoming normalized, action is needed to *return the rule of law* to the country’s response to terrorism. Significantly, the resources for this return are to be found in the current legal and political order. In sum, while the situation has certainly looked grim, there is ground for optimism.

The ground for optimism has of course only appeared firmer with the election of Barack Obama, who repeatedly voiced concerns over the Bush Administration’s conduct of the ‘War on Terror’ during his electoral campaign. Some eight months into office, President Obama appears to have chosen a course of action situated between the positions advocated by Cole and Lobel (2007) and Goldsmith (2007). His executive orders authorizing the immediate closure of the Central Intelligence Agency’s (CIA) secret prisons, the phased closure of the Guantanamo Bay Detention Camp, and the suspension of military tribunals at the camp (Shane 2009), as well as the more recent decision by United States Attorney General Eric Holder to appoint a special prosecutor to investigate allegations of torture by CIA interrogators (Meyer and Miller 2009), reflect a strategy to bring Bush-era policies back under the “rule of law.” His decision to replace CIA interrogators with the High Value Detainee Interrogation Group under the supervision of the National Security Council (NSC) reveals an attempt to alter, but not cease, Bush-era practices by housing them under a different institutional arrangement (Johnston 2009).

¹ Since the Bush Administration introduced the term “preemption” to describe its response to the September 11, 2001 terrorist attacks—first by Defense Secretary Donald Rumsfeld in Fall 2001, later by President Bush in his speech to West Point graduates in June 2002, and then more formally by the *National Security Strategy* report of September 2002 (Crawford 2005)—scholars have illustrated that the response possessed a “preventive” rather than “preemptive” logic. “Preemption involves striking now in the anticipation of an imminent adversary attack, with the aim of securing first-mover advantages. Prevention is a response to a future threat rather than an immediate threat” (Levy 2008, 4). While political scientists have largely considered this distinction with regard to discussions of “preventive war” and the legality of the US-led war against Iraq in 2003, others have located various elements of the Bush Administration’s counterterrorism efforts (detention of foreign nationals immediately following September 11, 2001, the extraordinary rendition of terrorist suspects to third-countries for coercive interrogation, the use of the Guantanamo Bay Detention Facility to house terrorist suspects, etc.) within a “preventive paradigm” (Lobel 2007).

² Of course not every commentator has viewed the Bush Administration’s policies as a departure from past precedent. John Yoo, who in his time working at the Office of Legal Counsel (OLC) authored various legal opinions that supported the implementation of controversial counterterrorism measures, and colleagues have argued that the Administration’s policies clearly follow upon examples set by past US Presidents responding to national security threats (Delahunty and Yoo 2009). Alan Dershowitz (2006), for his part, positions the Bush policies within a much longer history of “preemption” in both crime fighting and war making. The problem for Dershowitz is that the Western legal tradition never developed a “jurisprudence of preventive intervention” to regulate such actions.

In this paper, I present a different, less optimistic reading of the United States' 'War on Terrorism' by focusing on one element in this effort, the use of data mining technology to identify terrorist suspects. In simplest terms, the narrative I offer here can be read as a point-by-point refutation of the reformist view outlined above. Namely, while "data mining" and "preemption"³ might appear to represent a break with the past or from the norm, the tactics that the Bush Administration embraced in fighting terrorism are better read as *an extension* of a certain mode of future-oriented power, which Foucault (2008) referred to as "security" or "government," and which is symptomatic of (neo)liberal "risk society"⁴ (Amoore and de Goede 2008; Ericson and Haggerty 1996; Feeley and Simon 1992), that operates through the prediction of behavior and minimization of risk. Also, while civil liberties are no doubt at stake in this process, they are not at stake for everyone equally. Persons of Middle Eastern and North African (MENA) backgrounds have thus far borne the burden of the aggressive state response to the September 11 attacks (Mathur 2006; ACLU 2004; Volpp 2002), and it is reasonable to suspect that this discrimination will or has already become codified within the algorithms of data mining technology. Thus, *social justice* exists as a key concern. Finally, if the law promises the resources for reeling in the threats to civil liberties presented by the 'War on Terrorism,' it would not seem to offer the same for remedying the unequal burden of such threats. The War on Drugs, the policing of immigration, and past international disputes with 'terrorist regimes' have provided, borrowing from Simon (2007, 131), a "*crime jurisprudence*" that legitimizes such discrimination. From this view then, the ground for optimism appears fragile at best.

The paper is divided into 3 main sections. The first provides a brief overview of the use of data mining in counterterrorism efforts in the United States and the public concern that has emerged regarding the threat of government surveillance to privacy. The second section then moves to examine data mining from a different perspective, focusing on the technology's reliance upon profiling to consider its potential to codify discrimination against persons with MENA backgrounds. The third section reflects on the potential of the law to serve as a tool to combat such discrimination by reviewing past court decisions on racial, ethnic, and country-of-origin profiling. Finding few reasons for hope, the paper nonetheless concludes with a consideration of where the impetus for change might yet emerge.

Data Mining, Counterterrorism, and the 'Right to be Let Alone'

On December 16, 2005, *The New York Times* revealed that the US National Security Agency (NSA) was wiretapping telephone and email communications of people in the country in an effort to track individuals affiliated with Al-Qaeda (Risen and Lichtblau 2005). On May 11 of the following year, *The USA Today* reported that the NSA was actively collecting, with the cooperation of major telephone companies, the call records of millions of US citizens and residents in an effort to detect patterns of terrorist behavior (Cauley 2006). Together with earlier reports on government activities, such as the defunct Total Information Awareness (TIA) project (see Webb 2007), the stories highlighted the central role that surveillance⁵, and a particular type of surveillance named data mining, is playing in the US response to the September 11 terrorist attacks.

³ I use the term "preemption" here because of its popularity and connection to the Bush Administration. However, as noted in footnote 2, the Bush policy of "preemption" was actually one of "prevention."

⁴ 'Risk society' here carries the meaning intended by governmentality scholars—a society which uses "a probabilistic technique, whereby large numbers of events are sorted into a distribution, and the distribution in turn is used as a means of making predictions to reduce harm" in order to imagine and act upon problems (Rose, O'Malley, and Valverde 2006, 95). As Rose, O'Malley, and Valverde (2006, 95) explain, this notion of risk society is wholly different from that envisioned by Ulrich Beck (1992), who refers to post-industrial societies in which the risks engendered by scientific and technological processes have outgrown the capacity of those societies to control them.

⁵ Surveillance is defined as "any collection or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Lyon 2001:2).

Data mining is defined as “the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results” (GAO 2007, 4). Technically, data mining represents one step in a more general computational operation referred to as Knowledge Discovery in Databases⁶ (Fayyad, Piatetsky-Shapiro, and Smyth 1996), although the name has largely come to mean knowledge discovery itself in popular usage. And as a computational operation, data mining consists of three processes: “data input,” where data are collected, formatted, and stored in databases; “data analysis,” where data are queried using algorithms to find topics or patterns of interest⁷; and “results output,” where analysis outcomes are reported (GAO 2007, 4). Since September 11, the government has increasingly used data mining in its effort to prevent terrorism, as evidenced by such programs as the MATRIX⁸, TIA⁹, ADVISE¹⁰, TALON¹¹, and ATS¹², as well as the proliferation of “fusion centers” at the national, state, and local levels¹³.

⁶ Knowledge Discovery in Databases consists of a 9-part process according to Fayyad, Piatetsky-Shapiro, and Smyth (1996): 1. developing an understanding of the application domain; 2. creating a target data set; 3. data cleaning and preprocessing; 4. data reduction and projection; 5. matching the goals of KDD to a particular data mining method; 6. conducting an exploratory analysis; 7. data mining; 8. interpreting mined patterns; and 9. acting on the discovered knowledge (42). As noted above, the term ‘data mining,’ as used today, is understood to include most of these steps.

⁷ The most common methods of analysis in data mining are classification, regression, clustering, summarization, dependency modeling, and change and deviation detection (Fayyad, Piatetsky-Shapiro, and Smyth 1996, 44-45).

⁸ The MATRIX traces its origins to Hank Asher, a millionaire businessman who founded several companies dealing in electronic personal records. On September 13, 2001, Asher began work on a program to sift through his company’s (Seisint Inc.) databases in order to rate millions of people for terrorist potential. Within weeks, Asher’s program had produced a list of 120,000 names, which the company shared with the government. According to the company’s promotional materials, several arrests of persons with “High Terrorist Factor (HTF) scores” were then made (DeFede 2004, Webb 2007:153). Asher eventually sold his databases to the government, where they became the MATRIX (Multistate Antiterrorism Information Exchange), a network of state-administered databases subsidized by the Department of Homeland Security and the Justice Department that would help identify terrorism threats. In April 2005, amidst increasing public scrutiny concerning government surveillance, the federal government cut funding to the program, and it is now defunct.

⁹ The also ill-fated Total Information Awareness program (TIA) was begun by the newly-established Information Awareness Office (IAO) under the supervision of Dr. John Poindexter in 2002. The TIA program would have mined “individuals’ financial, medical, travel, ‘place/event entry,’ transportation, education, housing, and communications transactions” in order to “find ‘signatures’ of terrorist activity” (Webb 2007, 149). Though the TIA was eventually disbanded by the U.S. Congress in 2003, again amidst public concern, the program’s data mining activities reportedly continue in other projects referred to as “Evidence Extraction and Link Discovery” (Webb 2007, 150).

¹⁰ ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) was designed to allow the Department of Homeland Security (DHS) to sort through existing databases as well as incoming email texts, news articles, and other information sources so that analysts could establish relationships among different bits of information (GAO 2007, 2). ADVISE was terminated in September 2007 after it was discovered that tests of the program had used information from real people in violation of privacy requirements (Sniffen 2007).

¹¹ TALON (Threat and Local Observation Notice) was a program instituted by the Department of Defense following the 2001 terrorist attacks that collected and maintained information concerning suspicious persons and activities deemed to pose a threat to US service personnel and facilities. The program caught national attention once it was discovered that the TALON database contained information about antiwar activities (Lichtblau and Mazzetti 2006). Citing a lack of analytical value, the Defense Department decided to close the database, effective September 2007, although it would preserve the data “in accordance with intelligence oversight requirements” (Noyes 2007).

¹² ATS (Automated Targeting System) is maintained by the Customs and Border Protection (CBP) division of the Department of Homeland Security (DHS). It is designed to analyze disparate types of data in order to identify potential threats to security from people and materials crossing the country’s borders. As described by the Electronic Privacy Information Center (EPIC) (2006), citing the DHS’s own literature on the system, ATS assigns a risk profile “to all people ‘seeking to enter or exit the United States,’ ‘engag[ing] in any form of trade or other commercial transaction related to the importation or exportation of merchandise,’ ‘employed in any capacity related to the transit of merchandise intended to cross the United States border,’ and ‘serv[ing] as operators, crew, or passengers on any vessel, vehicle, aircraft, or train who enters or exits the United States.’” Unlike the other programs described in this section, ATS remains active, and controversial. Congressional appropriations bills have specified that funds cannot be used to “develop or test algorithms assigning risk to passengers whose names are not on government watch lists,” which would make the operation of ATS illegal (Singel 2006). DHS officials have responded however that the provisions in the appropriations bills are specific to the Secure Flight software operated by the United States Transportation Security Agency (TSA) and not ATS (see Singel 2006).

In counterterrorism applications, it is important to distinguish between “subject-based” and “pattern-based” analyses (Jonas and Harper 2006, 6; Popp and Poindexter 2006, 7). Subject-based analysis seeks to “trace links from known individuals or things to others”. Pattern-based analysis, meanwhile, uses “statistical probabilities to seek predicates in large data sets”. It “seeks to find new knowledge, not from the investigative and deductive process of following specific leads, but from statistical, inductive processes”. Because pattern-based analysis is characterized more by prediction than suspicion, it is also referred to as “predictive data mining” (Jonas and Harper 2006, 6). In the case of the NSA surveillance programs, for instance, the warrantless wiretapping program uncovered by the New York Times is an example of subject-based analysis, while the call record program reported by the USA Today is an example of pattern-based, predictive analysis¹⁴.

The revelation of the NSA surveillance programs, with the obvious allusions to Big Brother government, sparked both outrage and anxiety. State surveillance of citizens for suspicious activities is of course not novel in the United States, as evidenced by the Palmer Raids at the time of the First World War, the Red Scare of the 1950s, and the FBI’s COINTELPRO operations of the 1960s (Terkel 2007). However, it is precisely the familiarity with the past, and the legal battles that were won to limit such surveillance—the 1978 Foreign Intelligence Surveillance Act (FISA) for instance—that made the NSF programs seem such a radical departure from the norm. In this sense, *The New York Times* (2007) described the NSF’s domestic wiretapping as “A Spy Program in From the Cold,” meaning a program from the Cold War era.

For the most part, the discussion around government surveillance in the ‘War on Terrorism’ has centered on its threat to privacy. Reporters, for instance, have questioned whether the NSA’s warrantless wiretapping violates existing laws designed to protect privacy, such as the FISA and Title III of the 1968 Omnibus Crime Control and Safe Streets Act, which require the government to obtain warrants before monitoring personal communications (Nakashima 2007). Scholars have argued that new legislation enabling the government to mine personal data, such as Title II of the USA PATRIOT Act, entitled “Surveillance Procedures,” further erode 4th Amendment protections against “unreasonable searches and seizures” (Bloss 2007). And in view of such threats, they have called for changes to surveillance laws to better account for the “data retention” practices of the private sector (Bellia 2008); the adoption of a “proportionality principle,” where “the level of justification required for a search or seizure should be roughly proportionate to its intrusiveness” (Slobogin 2008); and greater “transparency in data mining programs” to ensure a balance between “liberty and security interests” (Solove 2008, Rubinstein, Lee, and Schwartz 2008). For good measure, government agencies themselves have expressed concern regarding the state’s use of data mining. In a recent report, the Government Accounting Office (GAO) (2007) enumerates a list of potential risks to privacy presented by data mining, including the potential for misidentification of individuals, information being used beyond the scope originally planned (which surveillance scholars refer to as “function creep” (Haggerty and Ericson 2006, 18)), and the security of information collected by the government (GAO 2007, 19).

¹³ Fusion centers are physical operation centers that, similar to the defunct TIA program and active ATS program, cull together information from a variety of sources—including information brokers such as LexisNexis (O’Harrow Jr. 2008)—in order to identify threats of different types. Unique from the other programs mentioned here, fusion centers operate at the local and state level, with over 70 fusion centers currently in operation (Hsu 2009). Given that they operate locally, the centers present a significant threat of “function creep.” In other words, despite being founded to prevent acts of terrorism, there is a great risk that they will expand their operations to include general crime-fighting (Monahan 2009). Interestingly, according to a recent report, state homeland security agencies have balked at provisions accompanying federal money that require them to focus their activities on specific terrorism-related concerns, such as threat assessments of improvised explosive devices (IEDs). The report notes that many state agencies “are trying to retool counterterrorism programs so that they focus more directly on combating gun violence, narcotics trafficking and gangs” (Schmitt and Johnston 2008). This tension would indicate that “function creep” has already set in at fusion centers, a fact attested to by former DHS Secretary Chertoff himself (see Schmitt and Johnston 2008). I return to the connections between counterterrorism and crime policy later in the article.

¹⁴ The later sections of this article will primarily focus on pattern-based data mining and its reliance on profiling to predict terrorist suspects.

To combat these threats to privacy, activists have turned to the courts. A number of lawsuits have challenged the legality of the NSA programs, although only a few of these remain active¹⁵. In addition, organizations such as the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) have helped file cases targeting other practices associated with counterterrorist data mining, such as the issuance of national security letters (NSL) to libraries seeking users' personal data (*Internet Archive et al. v. Mukasey et al.*), the US Customs and Border Protection's (CBP) policy of searching laptop computers "absent individualized suspicion" (*American Civil Liberties Union v. Department of Homeland Security*), and the government's use of individuals' cell phones as tracking devices (*American Civil Liberties Union v. Department of Justice*)¹⁶.

Court cases are critical, to be sure. But lost somewhat among the furor regarding government surveillance has been a fuller discussion about the value of privacy in our society. Many see privacy wed to freedom¹⁷. "The right to be let alone," which future Supreme Court Justice Brandeis outlined over a 100 years ago (Warren and Brandeis 1890), presents individuals unique opportunities to do as they please. This is of course a 'negative' reading of liberty—the absence of obstacles to one's actions—that "fails to provide much guidance about how privacy should be valued vis-à-vis other interests, such as free speech, effective law enforcement, and other important values" (Solove 2002, 1101). From a more 'positive' angle, others believe privacy provides the basis for a democratic society. "(P)rivacy is the foundation without which the freedoms of movement, association, assembly and speech cannot survive, and...without these freedoms, no resemblance of a public sphere can survive" (Fiske 1998, 79). The security of the private sphere allows individuals to come together to discuss social problems and elaborate strategies for remedying them. Without 'the private,' 'the public' cannot exist. And this, ultimately, is what is at stake in the government's surveillance programs.

¹⁵ The cases have named either the government or telecommunication companies cooperating with the NSF programs as defendants. Those naming the telecommunication companies as defendants have generally failed in the courts for various reasons, the most recent being the passage of the FISA Amendments Act in 2008, which granted the companies immunity from litigation. The most well-known of these cases, *Hepting vs. AT&T*, was rejected by Judge Vaughn Walker of United States District Court for the Northern District of California (N.D. Cal.) on June 3rd 2009 as a result of the FISA legislation. Interestingly, however, the *McMurray v. Verizon*, *AT&T*, and *BellSouth* case remains active. In this case, which broke off from the Hepting case, the plaintiffs allege that the passage of the FISA Amendments Act constitutes a violation of 5th Amendment due process rights, since it removed "a chance for a favorable judgment in a lawsuit that was already in progress" (Vaughan 2009). The cases naming the government as a defendant, meanwhile, remain active. The most interesting of these is probably the *Al Haramain v. Bush* case (also being heard by Judge Vaughn Walker of N.D. Cal) in which a Saudi Arabian charity organization alleges, based on a "top secret" document that the government mistakenly provided the group's lawyers, that the NSF illegally monitored its communications (Keefe 2008). Both the Bush and Obama Administrations have refused to provide the incriminating document to the court, claiming that such information is protected under the "state secrets" privilege (Kravets 2009a). Judge Walker has repeatedly threatened to issue a default judgment against the government (Kravets 2009b, Vaughan 2009). However, such a decision in favor of the plaintiffs could actually better serve the government, as it would prevent the court from establishing precedent on the executive power question at the heart of the lawsuit. The outcome of the case remains in limbo. Another case worth noting is *Jewel v. NSA*, which the Electronic Frontier Foundation (EFF) filed in response to the FISA Amendments Act. In place of suing the telecommunication companies, the EFF is now targeting the government for conducting surveillance without a warrant and certain government officials for authorizing the programs.

¹⁶ In *Internet Archive et al. v. Mukasey et al.*, the EFF and ACLU had filed a lawsuit challenging the Federal Bureau of Investigation's (FBI) issuance of a national security letter to the Internet Archive, a digital library. The letter requested personal information about one of the archive's users and prohibited the organization from acknowledging the existence of the letter. The case was settled in April 2008, with the FBI withdrawing the letter in question. In both *ACLU v. DHS* and *ACLU v. Department of Justice*, the ACLU has filed Freedom of Information Action (FOIA) requests seeking additional information about the practices in question. Both cases remain active (ACLU 2009).

¹⁷ Privacy involves much more than freedom, of course, though considerable disagreement exists about what that might be. In addition to the 'right to be let alone,' others have conceptualized privacy as limited access to personal information, the secrecy of personal information, an individual's ability to control access to personal information, personhood and respect for individuals' freedom to define themselves, and intimacy and respect for personal relationships (see Solove 2002). My interest here is not to decide upon a single definition of privacy, which is clearly difficult, but to consider the importance or function of privacy in society.

However, social theorists, critical legal scholars, and feminist scholars have been more critical of privacy (Gilliom 2001, 121-25). Privacy, they argue, is deeply enmeshed into relations of power and inequality in society. As John Fiske (1998) observes, “social power always involves the power not to be seen” (76). For example, the wealthy in US society invest considerable expense to create their own private space by constructing houses set apart from other residences and urban centers and individualized rooms within those homes that set family members apart from each other. They also fortify this space from ‘intruders’ through fences and high-tech surveillance systems. “The pauperized,” in contrast, lacking the resources that engender such a manipulation of space, “lack both external and internal privacy”¹⁸ (Fiske 1998, 76).

Similarly, privileging privacy often comes at the cost of recognizing competing social concerns. Until only very recently in the United States, domestic violence was an ‘invisible’ social problem because the law deemed the home a ‘private sphere’ to be insulated from social intrusions. As a result, women were left to endure and survive this systemic form of violence on their own (Pleck 1987). Along the same lines, in his intriguing study of low-income mothers contending with welfare surveillance, John Gilliom (2001) finds that the women seldom complain of their privacy being invaded. Rather, they are more concerned with the immense material needs facing them and their children. For those critical of privacy, such examples demonstrate a fundamental point, that privacy is an individualistic concern that encourages abandonment of social responsibility (see Gilliom 2001, 122).

Connecting back to counterterrorist data mining and government surveillance, the preceding line of thought pushes us to consider how the conflation of surveillance and privacy invasion has diverted our attention from other problematic dimensions of data mining. In the section that follows, I aim to counter this view by highlighting a particular feature of counterterrorist surveillance that, although less tangible to most than privacy, plays no less a role in defining the character of US society. This is data mining’s reliance on profiling.

Predictive Data Mining, Profiling in the ‘War on Terror’, and Social Justice

Companies have been using predictive, pattern-based data mining technology for years in order to better exploit “customer relationships” (Danna and Gandy 2002, 373, see also Fayyad, Piatetsky-Shapiro, and Smyth 1996, 38-39). Firms collect personal information from a diverse number of sites, including “call center, product registration, and point-of-sale transaction(s)” and internet-generated sources, such as “clickstream records,” on-line “shopping carts,” records of “entry and exit points” onto a website, and “search terms or key words” entered by website visitors (Danna and Gandy 2002, 374). They then analyze these data in an attempt to uncover patterns, associations, or rules that can characterize clients’ purchases or distinguish high value customers from low value ones (Gandy 2002, 5). For instance, using “neural network processing,” an example of a “classification” data mining method (Fayyad, Piatetsky-Shapiro, and Smyth 1996, 44), banks or insurance companies can analyze past records of bankruptcies or fraudulent claims to generate profiles that define and can predict high risk borrowers or dubious insurance claims in the future (Danna and Gandy 2002, 374). Alternatively, using “market basket analysis,” a type of “dependency modeling” method (Fayyad, Piatetsky-Shapiro, and Smyth 1996, 45), to identify which

¹⁸ It bears mentioning that a somewhat different conclusion is reached by others who have studied the experiences of high-income and low-income residents with surveillance. These authors (see Haggerty and Ericson 2006, 6, 2000, Marx 2005, Lyon 2001, 92) assert that the proliferation of surveillance in society has resulted in ‘synopticism’ (Mathieson 1997, 15), where the unprivileged many are able through mass media to keep constant watch of the privileged few. Similarly, in a more recent study comparing surveillance in a low-income housing project and high-income gated communities, Monahan (2006) finds that “remarkable similarities exist” between them, with residents of each site feeling subject to “undesired individual scrutiny and the policing of behaviors” (169-170). Nevertheless, and more in accord with the point concerning privacy argued above, residents in the high-income gated communities possess greater personal mobility and less risk for harsh sanction than their low-income counterparts (Monahan 2006, 169).

products are purchased together, online retailers can fit web shoppers into existing profiles in order to offer them “personalized content” during their visits to an online store (Danna and Gandy 2002, 375).

The outputs of such analyses can come to define new categories of consumers—“pools and patios,” “bohemian mix,” “urban achievers,” “blue blood estates,” “big city blues”—that firms can use to direct sales campaigns (Lyon 2003b, 23). When browsing an on-line shopping website, such as Amazon.com, the clickstream data that one generates is processed to match the user to such a category (Hanna and Gandy 2002, 375). By matching a shopper to existing profiles, the ‘e-tailer’ is able to showcase particular items or discounts associated with the profiles. The ‘personalized’ content that one encounters in the digital world, then, which produces an air of increasing individuality, is actually the result of putting people into generic ‘boxes’ (Hanna and Gandy 2002, 375).

Bearing these examples of predictive data mining’s business applications in mind, the government’s use of the technology can be seen not as a break with the past (although the decision to circumvent normal legal procedures to conduct the surveillance does appear to deviate from normal practice), but as an extension of a certain method for authorities to govern and manage populations. Where companies seek to collect and analyze data to categorize people for the sake of profit, the government has turned to collecting and analyzing data to categorize people for the sake of security.

And “security” is precisely the name Foucault (2008) gave to this technique. Unlike juridical power, which works “in the form of prohibition...along with its punishment,” and disciplinary power, which operates through “a series of supervisions, checks, inspections, and varied controls,” the future-oriented security apparatus “inserts the phenomenon in question...within a series of probable events” and “establishes a bandwidth of the acceptable that must not be exceeded” (Foucault 2008, 4-6). Following Foucault’s lead, governmentality scholars have gone on to trace the operation of this actuarial power in various incarnations in neoliberal society, in the “new penology” (Feeley and Simon 1992) at work in contemporary corrections, in the policing of the “risk society” (Ericson and Haggerty 1996), and in the general government of “freedom” in Western democracies (Rose 1999).

That counterterrorist data mining should find roots in the business world is interesting, since cost-value lies at the heart of security. Foucault (2008) notes, in elaborating his thoughts on security, that “the fundamental question is economics and the economic relation between the cost of repression and the cost of delinquency. Now what we see is that this problematic has led to such an inflation in disciplinary techniques, which were set up long ago however, that this increase of the disciplinary has been the point at which, if not scandal, at least friction has broken out” (9). Security, then, responds to the resistances engendered by discipline. To over-simplify the point, if the recalcitrant subject (be it a criminal, student, addict, or other) is not given to transform itself despite the application of expert knowledge and disciplinary techniques, then what authorities are left to do is to weed out such risks from the general circulation of legal, obedient, and healthy subjects, in order to allow for the “natural” growth of the latter (see Foucault 2008, 334-355). Such is the logic of the “Bush Doctrine,” which explicitly lists “the inability to deter a potential attacker,” along with “the immediacy of today’s threats” and “the magnitude of potential harm,” as a rationale for preventive action (see Delahunty and Yoo 2009, 844).

The application of predictive data mining to fight terrorism thus represents one step in a broader process of surveillance “intensification” (Wood, Konvitz, and Ball 2003, 137, Lyon 2003a) following 2001 that extends the operation of the “control society” into new spheres of social life (see Bogard 2006). Recent studies on surveillance have highlighted a number of problems accompanying this intensification. These include: an increasing problematization of personal identity, whether due to the multiplication of selves that results from surveillance technologies (Graham and Wood 2003) or the essentialization of personal identity via biometrical means (Ceyhan 2008, Bogard 2006, Amore and de Goede 2005); the increasing privatization of security operations without appropriate legal oversight (Boyne 2000); the

“presurveillance” or heightened social control that communities need implement to qualify for government funds for security technology (Fussey 2007); the normalization of intrusive surveillance procedures (Hall 2007); the de-skilling of security work (Ericson 1994) as well as complacency created therein due to an overreliance on technology (Marx 2001); the increased managerial control over employees at work (Monahan and Wall 2007), even amongst watchers employed in the surveillance industry (Smith 2007); and both the fallibility of surveillance technology (Haggerty 2006, Haggerty and Ericson 2006) and lack of qualified personnel at security agencies to operate such technologies (Manning 2008).

While these are all rightful concerns, what I want to focus on here is the possibility that race and ethnicity—specifically Middle Eastern and North African (MENA) background—will factor into the government's construction of terrorist profiles. Profiling, a term most often associated with the law enforcement practice of determining suspicious persons on the basis of racial and ethnic categories, is of course a sensitive topic. And up to now, the federal government has been vocal in its opposition to racial profiling in the 'War on Terror'. In the weeks following the September 11 attacks, President Bush held various meetings with Muslim and Sikh community leaders and strongly condemned the acts of violence perpetrated against Arab Americans, Muslims, and Sikhs following the attacks (US Department of Justice 2007). Title I of the USA PATRIOT Act also explicitly condemns such acts of violence, stating that “the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, must be protected, and that every effort must be taken to preserve their safety” and that “any acts of violence or discrimination against any Americans be condemned” (USA PATRIOT ACT 2001).

But however strenuously the President and Congress denounce targeting specific groups in retaliation for the September 11 attacks, the government's own actions indicate that racial profiling has been a primary means for conducting the 'War on Terror'. In the days following September 11, federal agents from the US Department of Justice “swept through Arab, Muslim, and South Asian neighborhoods throughout the country,” rounding up men for questioning in a program of preventive detention¹⁹ (ACLU 2004, 5). Shortly thereafter, the US Department of Justice sought to conduct some five thousand interviews with men from “Middle Eastern” or “Islamic” countries, who were not citizens of the US. Though the interviews were described as “voluntary,” some cooperating with the government's request were punished for minor visa violations (Volpp 2002, 1578). In June 2002, US Attorney General Ashcroft announced the creation of the National Security Entry Exit Registration System (NSEERS), requiring persons from certain countries—all of which were predominantly Arab or Muslim except for North Korea—to register with the program and be fingerprinted, photographed, and questioned (ACLU 2004, 6). Muslim-American students completing class assignments, meanwhile, have been detained for snapping photographs of government buildings (Schmitt 2009). And at US borders and airports, US Department of Homeland Security (DHS) Customs and Border Protection (CBP) agents continue to question Muslims, Arabs, and South Asian Americans “about their political beliefs, religious practices, and charities they support” (Muslim Advocates 2009).

These precedents suggest that the government would not be opposed to utilizing country of origin, religion, and ethnic background as bases for defining terrorist risk in its predictive data mining activities.

And while the secrecy surrounding the federal government's data mining programs (Nakashima 2009) prevents us from knowing how precisely ethnic background is factored into definitions of terrorists, technologists and other observers following the country's airport security systems firmly believe that ethnic and religious background do play a role in determining who to place on 'no-fly' lists or to stop for further questioning. To date, the US Transportation Security Agency (TSA) has developed different

¹⁹ As the ACLU study on the government's use of racial profiling notes, “Of the thousands of men who were detained and questioned, not one has been publicly charged with terrorism” (2004:5).

computer-based software systems to identify terrorist risks, including CAPPS (Computer Assisted Passenger Prescreening System), CAPPS II, and, now, Secure Flight (see Webb 2007, 150-60). In addition, US Customs and Border Protection (CBP) uses the ATS (Automated Targeting System) to assign risk scores to travelers passing through US borders (Singel 2006). Such programs generate assessments of an individual passenger's risk for terrorist activity by assigning specific values to particular characteristics, such as method of payment and type of ticket (round-trip versus one-way) (Lyon 2003a, 124-29). Congressional appropriations bills for DHS contain language prohibiting the development or testing of algorithms “assigning risk to passengers whose names are not on government watch lists,” but questions remain whether these restrictions apply to all DHS programs or solely Secure Flight²⁰ (Singel 2006). Those familiar with these programs not only believe that ethnicity and country of origin factor into the algorithms calculating terrorist risk, but that persons from a diverse background (read: Middle Eastern and Northern African background) would score so high that they could not avoid being stopped for extra questioning at the airport (see American Communications Foundation 2003 for a discussion on the efficacy of random versus profiling-based airport security systems). The ease with which one who lacks a MENA background can flout the airport security regime²¹ (Goldberg 2008), as well as the ongoing difficulties that Muslim, Arab, and South Asian Americans returning from abroad encounter at airports (Muslim Advocates 2009), provide some indication of the extent to which airport security personnel rely on mechanized assessments of passenger risk to do their work.

Thus, while there can be little doubt that counterterrorist data mining has invaded and will continue to invade individual privacy in the United States, these invasions of individual privacy will not be shared equally by all in society. Predictive data mining discriminates by design. It operates by designating certain groups as threats relative to others. As a consequence, persons with Middle Eastern and North African backgrounds will disproportionately bear the burden of this surveillance technique and the innumerable mistakes—false positives—that it will produce. In this sense, counterterrorist data mining threatens not just the legal protections individuals enjoy against state intrusion in the United States, which we might define as civil liberty, but also their fair distribution in society, which we might better call social justice.

The Law and Racial Profiling in the United States

On its face, racial profiling seems unconstitutional. By targeting groups of people for greater law enforcement scrutiny based on appearance rather than conduct, the practice would appear to violate both Fourth Amendment guarantees against “unreasonable searches and seizures” and Fourteenth Amendment guarantees to “equal protection” before the law. As such, one might hope that courts in the United States would provide relief to those suffering the discrimination of government counterterrorism surveillance.

However, there are reasons to be pessimistic. First, the supposed protections provided by the Constitution noted above and the power of the judiciary as a check to the power of the executive branch have steadily eroded over the past 40 years, as the United States has come to embrace “governing through crime” as a general model for political conduct (Simon 2007). To be certain, the 1960s witnessed a period of judicial activism—the Warren Court’s landmark decisions in *Map v. Ohio* (1961), *Gideon v. Wainwright* (1963),

²⁰ Prohibiting the application of risk-assessment algorithms to persons not already on government watch lists would effectively prohibit pattern-based, predictive data mining in the DHS. That is, if such algorithms can only be applied to people already on watch lists, the operation by definition is subject-based data mining—surveillance of those already suspected of terrorist links and activities. To this author’s knowledge, there has been no resolution to the question of whether the appropriations bills’ language applies only to Secure Flight or all DHS programs.

²¹ A November 2008 article in *The Atlantic* exhibits the ridiculous ways in which journalist Jeffrey Goldberg tested, and bested, airport security in the United States: carrying various weapons and terrorist paraphernalia onto flights, donning a “Beerbelly” polyurethane bladder to pass through security, and, most damningly, printing and boarding a plane using a fake boarding pass that he printed at home with the help of security-technology guru, Bruce Schneier. In conclusion, Goldberg refers to airport security in the country as “security theater,” measures put on “almost entirely for show” to make passengers feel more secure.

and *Miranda v. Arizona* (1966), for instance—that established strong standards protecting the procedural rights of suspects from abuses by the law enforcement community. Just as quickly however, and following the backlash provoked by these decisions, not to mention the civil unrest gripping the country in the late sixties, the Supreme Court reversed course, offering the *Terry v. Ohio* (1968) ruling that allows “stop and frisk” stops by officers. Conterminously, President Lyndon Johnson saw the passage of the Omnibus Crime Control and Safe Streets Act of 1968, ringing in the War on Crime that politicians of different ideological stripes have continuously sought to intensify in the pursuit of electoral victories. One result of this politico-legal shift in the United States has been the entrenchment of what Simon (2007) refers to as a “crime jurisprudence”, which is defined by the centrality of victims in the meaning of crime, a deference to the executive branch as representative of popular will, and a general pessimism about the role of courts in determining law enforcement matters (135-136). In such a setting, there is considerable reason to doubt the power of courts and the law to limit the government’s use of racial profiling in counter-terrorist data mining.

Indeed, US courts “have concluded that race can appropriately be used as a factor of suspicion in determining the likelihood that a person is engaging in, or has already committed, criminal behavior, so long as this use of race is *reasonably* related to law enforcement aims and not a mere pretext for racial harassment”²² [emphasis in original] (Kennedy 1998, 143). According to Randall Kennedy, courts define “‘reasonable’ racial profiling” against the backdrop of the “ugly realities” of “crime and its racial demographics” in the United States. Given historical forces and the structure of economic opportunities in the United States, studies have consistently shown that young Black men commit different types of street level crime at higher rates than the general population. In other instances, such as illegal immigration, the experience of law enforcement officers has shown that persons of “apparent Mexican ancestry” will transport undocumented aliens at higher rates than the general population. In this context, the courts have ruled, racial profiling is “reasonable” (Kennedy 1998, 144).

Implicit in these legal decisions is the idea of “balance,” that the law must “reflect a sensible balance between the social need for order and individuals’ desire for privacy and liberty.” In times of increased criminal activity then, “Fourth and Fifth Amendment rights” will vary (Stuntz 2002, 2138). And while racial profiling undoubtedly results in innocent people being stopped, the Supreme Court has opined that such stops, provided they are limited, represent reasonable costs for the benefits they provide in terms of public security (Kennedy 1999).

Some have already extended this line of reasoning to the ‘War on Terror’. K. Shiek Pal (2005), in a *Kennedy School Review* article entitled “Racial Profiling as a Preemptive Security Measure After September 11,” states that “(t)here will always be individual cases of false positives, but as long as the system works on the group level, that might be an acceptable and necessary consequence” (126). In a similar vein, Judge Richard Posner (2008) has more recently argued that criticisms of heightened surveillance practices are not “valid,” since the “cost of false positives must be balanced against that of false negatives” (252). So long as we are kept safe, the logic works, persons with MENA backgrounds might not mind the intrusion upon their constitutional rights.

²² In *Race, Crime, and the Law*, Kennedy reviews three court decisions establishing this principle (see Kennedy 1998, 140-4). In *State v. Dean*, the Arizona Supreme Court reasoned that Phoenix Police Department officers stopping a man because “he was a Mexican male in a predominantly white neighborhood” was “a practical aspect of good law enforcement”. In *United States v. Weaver*, the US Court of Appeals upheld the legality of the Drug Enforcement Agency (DEA) stopping a young black male debarking a flight from Los Angeles in Kansas City because he fit the profile of a gang member. The Court opined that, “Facts are not to be ignored simply because they may be unpleasant—and the unpleasant fact in this case is that [the DEA agent] had knowledge, based upon his own experience and upon the intelligence reports he had received from the Los Angeles authorities, that young male members of the black Los Angeles gangs were flooding the Kansas City area with cocaine.” Finally, on similar grounds, in *United States v. Martinez-Fuerte*, the US Supreme Court upheld the constitutionality of stopping motorists of “apparent Mexican ancestry” for suspicion of transporting undocumented aliens.

However reasonable these arguments might sound to some, they fail by their own logic. On the one hand, limits placed upon constitutional rights do not necessarily follow upon crime rates. Consider, for example, the Supreme Court's decision in *Board of Education of Independent School District No. 92 of Pottawatomie County v. Earls* (2002) described by Simon (2007, 16-17). In this case, the Board of Education in Pottawatomie County, Oklahoma had implemented a policy requiring any student participating in extra-curricular activities to submit to drug tests, even though no evidence of a drug problem existed in the school district. Students in the school district challenged the policy on 4th Amendment grounds, arguing that the policy violated their right to be secure "against unreasonable searches and seizures." Ultimately, the Supreme Court sided with the Board of Education, indicating in the process that fears of crime outweigh actual evidence of crime in determining the balance between individual liberties and state social control strategies. Likewise, fears of terrorism, rather than actual terrorist threats, may be deciding the balance between rights and security in the 'War on Terrorism.'

Of course, the attacks of September 11 did happen, and those attacks did involve persons from the Middle East. However, getting to the other hand, persons of "the so-called 'of Middle Eastern appearance' (OMEA) group" (Pal 2005, 119) do not disproportionately engage in terrorist activities relative to other groups in society. According to the US National Counterterrorism Center's (NCTC) Worldwide Incidents Tracking System (WITS), of all the acts of terrorism committed in the US and reported on the website, some 24 incidents over the last 5 years, none involves groups or persons related to 'radical Islam' (wits.nctc.gov). The groups most represented on the list are the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF), which target the facilities of those they allege cause harm to animals and the natural environment, as well as anti-abortion groups that target women's health clinics. On this basis, if the law enforcement community wished to utilize racial and ethnic profiling to stop acts of terrorism in the US, it would target persons 'of European appearance' who tend to make up such groups.

In addition to past Supreme Court rulings on racial profiling, there is a second reason to be pessimistic about the prospects of courts providing relief to persons from MENA communities suffering from profiling. This is the legal status of noncitizens. In an earlier period of profiling against persons from the Middle East—Iranians—following the seizure of over sixty US hostages in Teheran in 1979, US courts made a number of legal decisions establishing that "Congress and the Executive have enormous flexibility in decision-making related to immigration" (Mahdavi 2006, 217). From requiring Iranian university students studying in the US to submit special proof for continuing their student visas (*Narenji v. Civiletti*) to revoking deferred departure dates previously awarded Iranian nationals (*Yassini v. Crosland*), the courts allowed the government to single out particular groups in its application of immigration law (Mahdavi 2006, 217-18, see also Johnson 2004, n67 for additional cases involving Iranian immigrants).

In the current 'War on Terrorism', this distinction between citizen and noncitizen is perhaps most strikingly drawn in the US Department of Justice document, "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," published by the department's Civil Rights Division. In it, the government expresses its clear opposition to racial profiling in "traditional law enforcement activities," noting "race cannot be considered in a traffic stop or other investigatory activity unless it has been reported that the perpetrator of a crime is of a particular race" (US Department of Justice 2003). However, the document carefully distinguishes "traditional law enforcement activities" from "national security and border integrity" activities and states that "(f)ederal law enforcement officers who are protecting national security or preventing catastrophic events (as well as airport security screeners) *may* consider race, ethnicity, and other relevant factors to the extent permitted by our laws and the Constitution" [emphasis added] (US Department of Justice 2003). And as the preceding paragraphs demonstrate, the courts have provided considerable latitude for using such factors in determining whom to place under increased surveillance.

Of course, such contradictions simply evidence the racial politics at work in the ‘War on Terrorism.’ As Leti Volpp (2002) writes, the attack on the Oklahoma City federal building in 1995 did not precipitate an era of racial profiling against Whites, and “Timothy McVeigh did not produce a discourse about good whites and bad whites, because we [White society] think of him as an individual deviant, a bad actor. We do not think of his actions as representative of an entire racial group” (1585).

Implicit here as well are competing ideas concerning victimhood. In “crime jurisprudence,” the victim occupies a privileged position, as “it is in the experience of victimization, and, much more commonly, the imagined possibility of victimization, that the political community and its governable interests are being redefined” (Simon 2007, 109). In theory, the imagined victim in the ‘War on Terrorism’ is not clear. That is, is it the person of MENA descent who would have his civil rights violated by an over-zealous (state) security apparatus? Or is it the person of European descent who would be the victim of terrorist attacks? Of course, in practice, the imagined victim is never in doubt. And it will be the person of MENA descent who will have to endure the pains of victimization for the imagined security of the White majority.

To review then, predictive counterterrorist data mining will, by design, place additional burdens on persons from MENA communities. In placing this group of individuals under increased surveillance without evidence of wrongdoing, data mining threatens Constitutional guarantees to liberty and justice. However, given the state of public and legal opinion in the United States regarding the use of racial profiling, there is little reason to expect the law to provide relief to those suffering from this injustice.

Conclusion: America Through the Looking Glass

‘Nothing will ever be the same after September 11’ is an often repeated and widely accepted idea in the United States. However, as Slavoj Žižek (2002) observes, the phrase is “never further elaborated—it is just an empty gesture of saying something ‘deep’ without really knowing what we want to say” (46). For many critical of the US government's response to the attacks, the phrase suggests a break with the past, a fork in the road between a past where the United States represented a model of freedom and justice and a future where those principles are in decline. Increased government surveillance in general, and counterterrorist data mining in particular, are key exhibits evidencing this break. To mend this breach, the Obama Administration would need either return to the rules of old (Cole and Lobel 2007) or create new institutions (Goldsmith 2007) and political arrangements (Ackerman 2006) to better manage the threat of terrorism.

However, as the example of predictive data mining demonstrates, the US response to the terrorist attacks of September 11 might be better read as an intensification of, rather than break with, the past. Dimensions of injustice that defined the founding of the country and its continued governance have been expanded and newly elaborated. ‘Preemption’ is not a novel doctrine authored by the Bush Administration, but a constituent part of the “security dispositif” through which risks can be managed and (neo)liberal governance can come to life (Foucault 2008, 48-49). Domestically, African Americans, Latinos, and other minority groups in the United States have long experienced the injustices accompanying state strategies designed to keep society safe, whether the threats imagined were drugs, gang violence, labor unrest, or American identity itself. The use of data mining to surveil Middle Eastern and North African communities represents a reformulation of this strategy of social control through digitized means. To the extent that such policing has in the past largely been conducted within, or come to define, the boundaries of the law (Simon 2007), it is difficult to see the rule of law as an adequate resource for answering the problem of profiling in the ‘War on Terrorism’.

The point here is not to simply be contrarian. The popular discontent with the Bush Administration’s response to the September 11 attacks has provided a unique opportunity to reshape the government’s counterterrorism policies and reimagine its relation to the people. Given this moment, defining the

challenge before us as precisely and earnestly as possible is critical. And to name the problem as one primarily concerning civil liberties is to define the problem in a conservative manner that will invite simple solutions which, if allaying the inquietudes of the majority, fail to address the root of the problem.

So then, what are the answers? Speaking to the problem of racial profiling in general, Randall Kennedy (1999) has proposed to simply outlaw the practice and to compensate for the resulting loss in police intelligence by putting additional law enforcement officers on the street and/or increasing the scrutiny of everyone in society (34). Bruce Ackerman (2006), who proposes using short-term “quarantines” of suspicious persons as part of his “emergency constitution,” suggests compensating innocent people detained following a terrorist attack on the order of \$500 a day (47-55). These are clearly two distinct ways of addressing the issue. The former aims to eliminate the practice completely by increasing state surveillance upon all, while the latter proposes to rationalize its continued existence. The two proposals coincide however in judging profiling as wrong and proposing to address this wrong by increasing the burdens upon the whole of society, whether through increased surveillance or increased public funds to compensate victims.

What the proposals also share is the assumption that the political will necessary to pass such legislation—the majority willingly placing new burdens upon itself for the sake of minorities—could actually appear. From a sociological perspective, the prospects of such a political consensus emerging appear doubtful, considering the extent to which major social institutions now rely on digitized forms of sorting and profiling to operate. Thus, one finds it difficult to be optimistic about the possibilities for change in the control society.

But “it is sad and distressing to live without hope,” Dostoyevsky once remarked (Pereverzev 1925). And to conclude this paper, I can suggest that hope in this case might emerge from one of two sources. First, to revisit Kennedy’s (1999) work, he contends that one of the chief harms of racial profiling is its effects on state legitimacy. By placing African American communities under increased scrutiny, the police have earned the resentment of those communities, who come to question the legitimacy of the law. And such distrust, to the extent that it diminishes people’s cooperation with police investigations and other police work, hampers law enforcement. In an increasingly multicultural country, a mode of governance that relies on keeping certain groups under surveillance and limiting their civil liberties may simply become untenable. As data mining and other surveillance technologies are increasingly deployed in the ‘War on Terror,’ and the number of suspicious persons increases, so too might the public’s suspicion of the law (Levi and Wall 2004, 209). And if the country’s leaders are unable to correct such an unjust system of rule, one could expect the resulting crisis of legitimacy to correct the system itself.

Second, before such a crisis results, perhaps the political leadership necessary to create change might yet emerge. If Harold and Kumar, respectively of Korean and Indian origin, can break through the Hollywood color barrier to chase the adolescent dreams traditionally circulated in the currency of White male subjects, perhaps something truly is afoot in the United States. With this in mind, it is right that we should take hope not only in the fact that George W. Bush has left office, ostensibly restoring the country to its prior course, but that an African American man who spent years of his childhood in a Muslim country has taken his place.

To date, President Obama has been ambiguous in his stance towards Bush Administration policies in the ‘War on Terror.’ On the campaign trail, he took a clear position in opposition to his predecessor. And in office, he has signed executive orders to close the Guantanamo Bay Detention Camp and the CIA’s secret prisons around the world (Shane 2009) and has seen his Attorney General assign a special prosecutor to investigate allegations that the CIA tortured prisoners during interrogations (Meyer and Miller 2009). At the same time, however, not only has President Obama continued the programs of rendition of US prisoners to third countries for the purposes of interrogation and incarceration (Johnston 2009) and using

military tribunals at Guantanamo Bay to try suspected terrorists (Glaberson 2009), but so too has he continued the NSA's surveillance programs, which are now legally protected under the FISA Amendments Act (Bamford 2009).

In a certain light, this ambivalence from the new President mirrors that present in Harold and Kumar. Harold, the more reticent of the pair, continually makes efforts to fit himself into the established social order (working as a banker, dressing conservatively, and taking pains to ingratiate himself with his more successful colleagues), even while he flirts with the alternative lifestyle so enthusiastically embraced by his friend Kumar (smoking marijuana abundantly, preoccupying himself with sex, and not doing what others want him to do, such as becoming a medical doctor). Inevitably, Harold's efforts fail, due to the intractable chauvinism of those White characters sitting in positions of power and privilege. And he is in the end brought closer to Kumar. To conclude then, as President Obama continues seek the middle ground in a polity that openly questions his US citizenship and likens his socially-minded policies to National Socialism, we might hope that he has a Harold-moment of his own and uses the extraordinary authority that "crime jurisprudence" has placed in the Office of the US Presidency to push the country onto a progressive path that would truly represent a break with the past.

Acknowledgements

Earlier versions of this article were presented at the Second International Conference sponsored by the Center for American Studies and Research at American University of Beirut in December 2007, a Faculty Forum meeting at Bloomfield College in April 2008, and the Annual Meeting of the Law and Society Association in Montreal in May 2008. The author thanks David Murakami Wood, Allen Hibbard, Daniel Skinner, Esmail Najmi, Richard Hart, Thomas Slaughter, Sharryn Aiken, Beth Ribet, Andrew Pickering, and two anonymous reviewers for helpful comments that guided revisions.

References

- Ackerman, Bruce. 2006. *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism*. New Haven, CT: Yale University Press.
- American Civil Liberties Union (ACLU). 2004. *Sanctioned Bias: Racial Profiling Since 9/11*. New York: ACLU National Headquarters.
- ACLU. 2009. Safe and Free: Court Cases. Available at: http://www.aclu.org/safefree/relatedinformation_court_cases.html
- American Communications Foundation. 2003. Random Security. *ACFNewsSource*. Available at: http://www.acfnewsSource.org/science/random_security.html
- Amoore, Louise and Marieke de Goede. 2008. Governing by Risk in the War on Terror. In *Risk and the War on Terror*, eds. Louise Amoore and Marieke de Goede, 5-19. New York: Routledge.
- Amoore, Louise and Marieke de Goede. 2005. Governance, Risk, and Dataveillance in the War on Terror. *Crime, Law, and Social Change* 43: 149-173.
- Bamford, James. 2009. The NSA is Still Spying on You. Available at www.salon.com.
- Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity* [transl. Mark Ritter]. London: Sage Publications.
- Bellia, Patricia. 2008. The Memory Gap in Surveillance Law. *The University of Chicago Law Review* 75: 137-179.
- Bloss, William. 2007. Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects. *Surveillance and Society* 4(3): 208-228.
- Bogard, William. 2006. Welcome to the Society of Control: The Simulation of Surveillance Revisited. In *The New Politics of Surveillance and Visibility*, ed. Kevin Haggerty and Richard Ericson, 55-78. Toronto: University of Toronto Press.
- Boyne, Roy. 2000. Post-Panopticism. *Economy and Society* 29(2): 285-307.
- Broache, Anne. 2007. Appeals Court Dismisses Suit Against NSA Spy Program. *c-net news.com*, July 6. (retrieved July 15, 2007).
- Cauley, Leslie. 2006. NSA Has Massive Database of Americans' Phone Calls. *USA Today* May 11, 2006.
- Ceyhan, Ayse. 2008. Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance and Society* 5(2): 102-123.
- Cole, David and Jules Lobel. 2007. *Less Safe, Less Free: Why America is Losing the War on Terror*. New York: The New Press.
- Crawford, Neta. 2005. The Justice of Preemption and Preventive War Doctrines. In *Just War Theory: A Reappraisal*, ed. Mark Evans, 25-49. Edinburgh: Edinburgh University Press.
- Danna, Anthony and Oscar H. Gandy, Jr. 2002. All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. *Journal of Business Ethics* 40: 373-386.
- DeFede, Jim. 2004. Mining the Matrix. *Mother Jones*, September/October.

- Delahunty, Robert and John Yoo. 2009. The "Bush Doctrine": Can Preventive War Be Justified? *Harvard Journal of Law and Public Policy* 32: 843-865.
- Dershowitz, Alan. 2006. *Preemption: A Knife That Cuts Both Ways*. New York: W.W. Norton and Company.
- Electronic Privacy Information Center (EPIC). 2006. Customs and Border Protection's Automated System Targets U.S. Citizens. Available at: <http://epic.org/privacy/surveillance/spotlight/1006>
- Ericson, Richard. 1994. The Division of Expert Knowledge in Policing and Security. *British Journal of Sociology* 45(2): 149-175.
- Ericson, Richard and Kevin Haggerty. 1996. *Policing the Risk Society*. Toronto: University of Toronto Press.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 1996. From Data Mining to Knowledge Discovery in Databases. *AI Magazine* Fall: 37-51.
- Feeley, Malcolm and Jonathon Simon. 1992. The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology* 30(4): 449-474.
- Fiske, John. 1998. Surveilling the City: Whiteness, the Black Man, and Democratic Totalitarianism. *Theory, Culture, and Society* 15(2): 67-88.
- Foucault, Michel. 2008. *Security, Territory, Population: Lectures at the College de France, 1977-1978*. New York: Picador.
- Fussey, Pete. 2007. An Interrupted Transmission? Processes of CCTV Implementation and the Impact of Human Agency. *Surveillance and Society* 4(3): 229-256.
- Gandy, Oscar H. 2002. Data Mining and Surveillance in the Post-9.11 Environment, presented at the Political Economy Section, IAMCR, Barcelona, July.
- Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.
- Glaberson, William. 2009. U.S. May Revive Guantánamo Military Courts. *The New York Times*, May 2.
- Goldberg, Jeffrey. 2008. The Things He Carried. *The Atlantic*, November.
- Goldsmith, Jack. 2007. *The Terror Presidency: Law and Judgment Inside the Bush Administration*. New York: W.W. Norton & Company.
- Goldsmith, Jack. 2008. Fixing It: The Law in Wartime. Available at: <http://www.slate.com/id/2187870/>.
- Government Accounting Office (GAO). 2007. *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*. GAO-07-293. Washington, D.C.
- Graham, Stephen and David Wood. 2003. Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy* 23(2): 235-256.
- Haggerty, Kevin. 2006. Visible War: Surveillance, Speed, and Information War. In *The New Politics of Surveillance and Visibility*, ed. Kevin Haggerty and Richard Ericson, 250-277. Toronto: University of Toronto Press.
- Haggerty, Kevin and Richard Ericson. 2006. The New Politics of Surveillance and Visibility. In *The New Politics of Surveillance and Visibility*, ed. Kevin Haggerty and Richard Ericson, 3-33. Toronto: University of Toronto Press.
- Haggerty, Kevin and Richard Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 1(51): 605-622.
- Hall, Rachel. 2007. Of Ziploc Bags and Black Holes: The Aesthetics of Transparency in the War on Terror. *The Communication Review* 10: 319-346.
- Hsu, Spencer. 2009. Security Chief Urges 'Collective Fight' Against Terrorism. *The Washington Post*, July 29.
- Johnson, Kevin. 2004. Racial Profiling After September 11: The Department of Justice's 2003 Guidelines. *Loyola Law Review* 50: 67-87.
- Johnston, David. 2009. U.S. Says Rendition to Continue, but With More Oversight. *The New York Times*, August 25.
- Jonas, Jeff and Jim Harper. 2006. Effective Counterterrorism and the Limited Role of Predictive Data Mining. *Cato Institute Policy Analysis* no.584, December 11.
- Keefe, Patrick Radden. 2008. State Secrets: A Government Misstep in a Wiretapping Case. *The New Yorker*, April 28.
- Kennedy, Randall. 1998. *Race, Crime, and the Law*. New York: Vintage Books.
- Kennedy, Randall. 1999. Suspect Policy. *The New Republic*, September 13&20.
- Kravets, David. 2009a. Obama Says Government Sanctions Unwarranted in Spy Case. Available at www.wired.com
- Kravets, David. 2009b. Obama Claims Immunity, As New Spy Case Takes Center Stage. Available at www.wired.com
- Levi, Michael and David S. Wall. 2004. Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, 31(2): 194-220.
- Levy, Jack. 2008. Preventive War and Democratic Politics. *International Studies Quarterly* 52: 1-24.
- Lichtblau, Eric and Mark Mazzetti. 2006. Military Documents Hold Tips on Antiwar Activities. *The New York Times*, November 21.
- Lobel, Jules. 2007. The Preventive Paradigm and the Perils of Ad Hoc Balancing. *Minnesota Law Review* 91: 1407-1450.
- Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK: Open University Press.
- Lyon, David. 2003a. *Surveillance after September 11*. Cambridge, UK: Polity Press.
- Lyon, David. 2003b. Surveillance after September 11, 2001. In *The Intensification of Surveillance: Crime, Terrorism, and Warfare in the Information Age*, ed. Kirstie Ball and Frank Webster, 16-25. London: Pluto Press.
- Mahdavi, Sara. 2006. Held Hostage: Identity Citizenship of Iranian Americans. *Texas Journal on Civil Liberties and Civil Rights* 11(2): 211-44.
- Manning, Peter. 2008. *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press.

- Marx, Gary T. 2001. Technology and Social Control. In *International Encyclopedia of the Social and Behavioral Sciences*, ed. Neil Smelser and Paul Baltes. St. Louis, MO: Elsevier.
- Marx, Gary T. 2005. Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies. *Law and Social Inquiry* 30(2): 339-399.
- Marx, Gary T. 2004. What's New about the 'New Surveillance'? Classifying for Change and Continuity. *Surveillance & Society* 1(1): 9-29.
- Mathieson, Thomas. 1997. The Viewer Society: Michel Foucault's 'Panopticon' Revisited. *Theoretical Criminology* 1(2): 215-234.
- Mathur, Shubh. 2006. Surviving the Dragnet: 'Special Interest' Detainees in the US after 9/11. *Race and Class* 47(3): 31-46.
- Meyer, Josh and Greg Miller. 2009. Holder Open Investigation into CIA Interrogations. *The Los Angeles Times*, August 25.
- Monahan, Torin. 2006. Electronic Fortification in Phoenix: Surveillance Technologies and Social Regulation in Residential Communities. *Urban Affairs Review* 42(2): 169-192.
- Monahan, Torin. 2009. The Murky World of 'Fusion Centers'. *Criminal Justice Matters* 75: 20-21.
- Monahan, Torin and Tyler Wall. 2007. Somatic Surveillance: Corporeal Control through Information Networks. *Surveillance and Society* 4(3): 154-173.
- Muslim Advocates. 2009. Unreasonable Intrusions: Investigating the Politics, Faith, & Finances of Americans Returning Home. Available at: <http://www.muslimadvocates.org>
- Nakashima, Ellen. 2007. The Legal Tangles of Data Collection. *The Washington Post*, January 16, A09.
- Nakashima, Ellen. 2009. Administration Seeks to Keep Terror Watch-List Data Secret. *The Washington Post*, September 6.
- The New York Times*. 2007. Editorial: A Spy Program in from the Cold, January 18.
- Noyes, Andrew. 2007. Civil Libertarians Laud End to TALON Surveillance. *National Journal*, August 21.
- O'Harrow Jr., Robert. 2008. Centers Tap Into Personal Databases. *The Washington Post*, April 2.
- Pal, K. Shiek. 2005. Racial Profiling as a Preemptive Security Measure After September 11: A Suggested Framework for Analysis. *Kennedy School Review* Spring 2005: 119-129.
- Pereverzev, Valerian. 1925. *F. M. Dostoevsky*, Moscow.
- Pleck, Elizabeth. 1987. *Domestic Tyranny: The Making of American Social Policy Against Family Violence from Colonial Times to the Present*. New York: Oxford University Press.
- Popp, Robert and John Poindexter. 2006. Countering Terrorism through Information and Privacy Protection Technologies. *IEEE Security and Privacy* 4(6): 18-27.
- Posner, Richard. 2008. Privacy, Surveillance, and Law. *The University of Chicago Law Review* 75: 245-260.
- Risen, James and Eric Lichtblau. 2005. Bush Lets U.S. Spy on Callers Without Courts. *The New York Times*, December 16.
- Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*, New York: Cambridge University Press.
- Rose, Nikolas, Pat O'Malley, and Mariana Valverde. 2006. Governmentality. *Annual Review of Law and Social Science* 2: 83-104.
- Rubinstein, Ira, Ronald Lee, and Paul Schwartz. 2008. Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review* 75: 261-285.
- Schmitt, Eric. 2009. Surveillance Effort Draws Civil Liberties Concern. *The New York Times*, April 29.
- Schmitt, Eric and David Johnston. 2008. States Chafing at U.S. Focus on Terrorism. *The New York Times*, May 26.
- Shane, Scott. 2009. Obama Orders Secret Prisons and Detention Camps Closed. *The New York Times*, January 23.
- Simon, Jonathan. 2007. *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. New York: Oxford University Press.
- Singel, Ryan. 2006. DHS Passenger Scoring Illegal? Available at: <http://www.wired.com>
- Slobogin, Christopher. 2008. Government Data Mining and the Fourth Amendment. *The University of Chicago Law Review* 75: 317-342.
- Smith, Gavin J.D. 2007. Exploring Relations between Watchers and Watched in Control(led) Systems: Strategies and Tactics. *Surveillance and Society* 4(4): 280-313.
- Sniffen, Michael. 2007. Homeland Security Drops Data-Mining Tool. *Associated Press*, September 6.
- Solove, Daniel. 2002. Conceptualizing Privacy. *California Law Review* 90: 1087-1155.
- Solove, Daniel. 2008. Data Mining and the Security-Liberty Debate. *The University of Chicago Law Review* 75: 343-362.
- Stuntz, William. 2002. Local Policing After the Terror. *Yale Law Journal* 111: 2137-2194.
- Terkel, Studs. 2007. The Wiretap This Time. *The New York Times*, October 29.
- United States Department of Justice. 2007. Presidential Remarks, available at: <http://www.usdoj.gov/crt/legalinfo/bushremarks.html>
- United States Department of Justice. 2003. Guidance Regarding the Use of Race By Federal Law Enforcement Agencies, Available at: http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm
- USA PATRIOT ACT. 2001. United States Congress Public Law No. 107-56.
- Vaughan, Susan. 2009. Federal Judge Issues Mixed Rulings in Warrantless Wiretapping Cases. Available at <http://www.fogcityjournal.com>
- Volpp, Leti. 2002. The Citizen and the Terrorist. *UCLA Law Review* 49: 1575-1599.
- Warren, Samuel and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4: 193.
- Webb, Maureen. 2007. *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*. San Francisco: City Lights Books.

- Wood, David, Eli Konvitz and Kirstie Ball. 2003. The Constant State of Emergency? Surveillance after 9/11. In *The Intensification of Surveillance: Crime, Terrorism, and Warfare in the Information Age*, ed. Kirstie Ball and Frank Webster, 137-150. London: Pluto Press.
- Žižek, Slavoj. 2002. *Welcome to the Desert of the Real: Five Essays on September 11 and Related Dates*. New York: Verso.